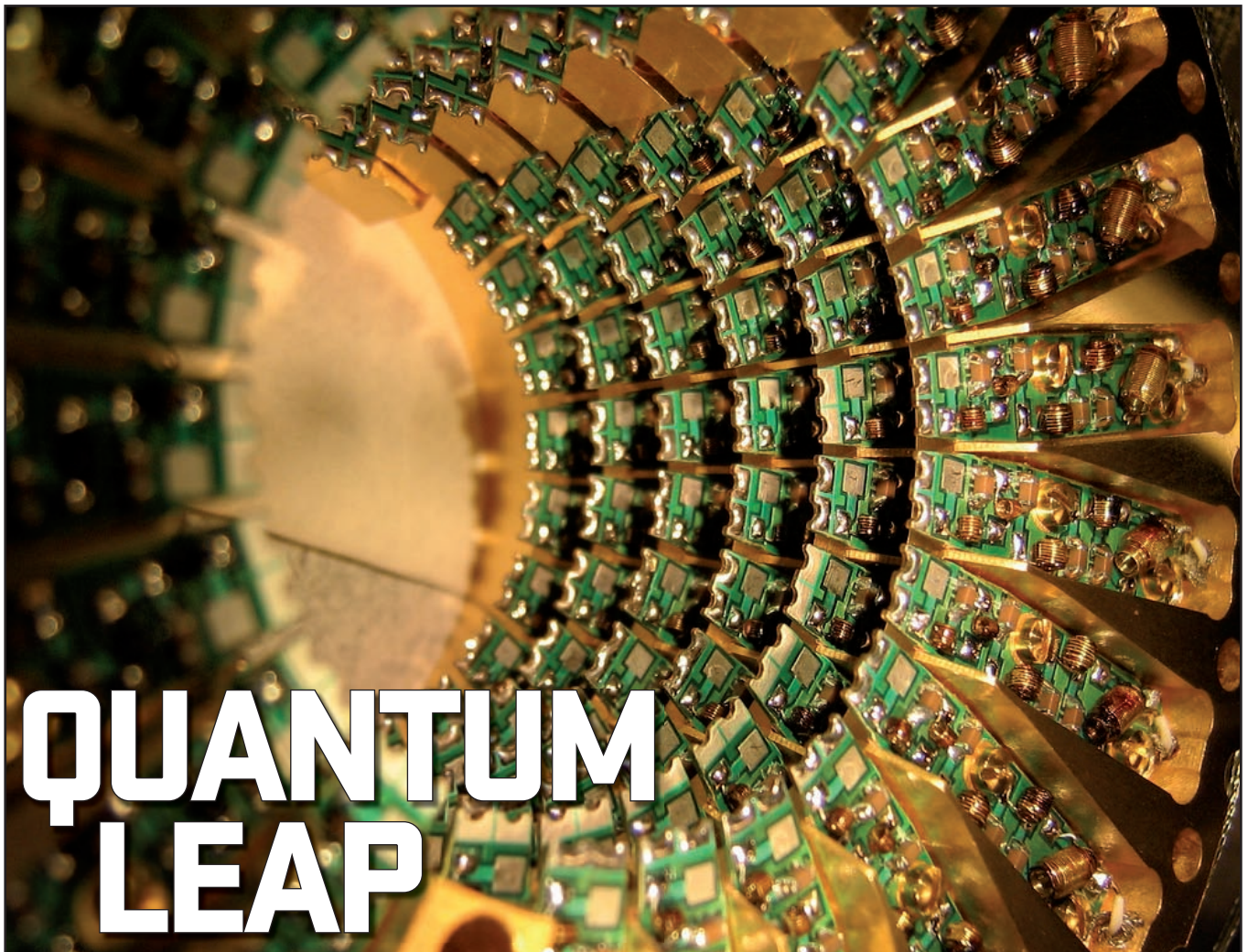




QUANTUM LEAP

Quantum mechanics describe a pretty freaky universe, but one company claims to have built a computer that harnesses its power. Peter Judge finds out more

Quantum computing sounds like the stuff of fantasy. It proposes machines that operate much faster than any current computer because they can carry out thousands of calculations at the same time in parallel universes.

Computing ideas really don't come more bizarre than that, and yet one company claims to have taken a big step towards making this a reality, and hopes to have commercial quantum computers in server rooms within the next couple of years. To find out if that could possibly be true, we'll look at the basic ideas of how to make a computer that uses quantum principles.

SIMPLE QUANTUM PHYSICS

First, let's throw out the quantum myths. Despite what you've heard, quantum mechanics is not hard to understand, it's not controversial and it doesn't overturn all the previous laws of physics.

Physicist and Nobel laureate Richard Feynman said that nobody understands quantum mechanics – but is this true? The basic principles were worked out in the first half of the last century. By the 1970s, physics students had text books with titles such as *Simple Quantum Physics*. Now it's on the A-level syllabus. When it comes down to it, quantum behaviour is no more mysterious than any other part of physics.

The fundamentals of quantum mechanics aren't controversial, either. Around 1900,

scientists looking at tiny particles saw effects that conventional physics couldn't explain. They developed theories that explained those effects. The theories were surprising, but they fit the facts exactly, and correctly predicted the results of new experiments. The scientific establishment adopted them. They've been tweaked and revised, but they're still in use.

Quantum mechanics improved on existing science, but it didn't consign conventional science to the dustbin. It is a more fundamental explanation of the universe than classical physics. It explains things at the level of atoms and electrons that no other theory can explain.

For instance, every particle can also be described as a wave. It's not one or the other – it's both. Even more freakily, until you observe it, every particle can be in several places at once.

Light, for instance, is a wave, but it's also a particle. The wavelength dictates the colour, and prisms bend it, but physical processes give out light in measurable chunks, called photons.

The well-known double-slit experiment shows quantum mechanics in action. Around 1800, English scientist Thomas Young used it to prove that light was a wave. If you shine a light at a plate with two slits in it, the light spreads out (diffracts) on the far side. On a screen, light and dark interference fringes can be seen; in some places the light adds up, and in others it subtracts because it is out of phase.

In 1961, Claus Jönsson of the University of Tübingen carried out the same experiment with electrons rather than light. These were known to be particles, but the two-slit experiment proved that electrons were also waves.

Pier Giorgio Merli at the University of Milan did a similar experiment in 1974 with sensitive equipment that let him send one electron through the slits at a time. The interaction still happened. Electrons popped up on the screen one by one, but over time they built up into the same interference pattern. In other words, each electron went through both slits, and interfered with itself. It was in two places at once.

Until it interacts with other particles, all the possible states of a particle are 'superposed', and the system is 'coherent'. When it interacts with another particle, it 'decoheres' and settles into one of the possible states. Which one it chooses is a matter of probability, and those probabilities are determined by a mathematical expression called the wave function.

In another quantum effect, called entanglement, two particles are connected so that the state of one depends on the other.

You don't often see these quantum effects in the everyday world. Real-world objects contain billions of particles, and they aren't isolated. They are not in a coherent quantum state, so Newton's laws still do a better job of explaining the real world than quantum mechanics.



QUANTUM COMPUTING

Irwin Schrodinger imagined a real-world quantum system in his famous cat paradox. Imagine a cat in a box with a cylinder of poison gas, the valve of which is controlled by the quantum state of a single particle. If it's isolated from the rest of the world, it's a quantum system. We don't know what state the particle is in and therefore we don't know if the valve is open or closed, or whether the cat is alive or dead. Until we open the box, there are two 'superposed' cats, one alive and one dead.

This is just a theoretical experiment. In a real box there would always be interaction between the cat and the outside world. This could be as small as a quantum of heat slipping out, or a sound getting in. Any interaction would decohere the particles in the box. Schrodinger's cat is a theoretical puzzle, not a science project.

That is, until the quantum computing idea was floated. At its simplest, quantum computing is a version of Schrodinger's cat experiment.

THE BASIC IDEA

The idea of quantum computing was suggested by Richard Feynman and Paul Benioff, but its real father was David Deutsch, who spelt out the possibility in 1985, and started to work out algorithms that might be useful on a quantum computer. Since then, theoreticians have put meat on the bones, and researchers have built prototypes of quantum computing components.

Imagine a computer that has a set of inputs to process. For each possible input, the computer is in a different quantum state. If you can isolate the system, all those multiple states exist at the same time, and the computer can process every possible input at the same time.

In effect, a quantum computer is multiple computers superposed. One quantum bit, or qubit, lets the machine make two calculations at a time, and each additional qubit doubles the number of inputs, and the number of virtual computers. A quantum computer with just 300 qubits would be like 10^{90} conventional computers – more than the number of atoms in the known universe.

This speed-up is beyond anything you can get by squeezing more components on a piece of silicon or speeding up the processor's clock. That just adds more bits to the capacity of the system or lets it do more calculations in a given time. A quantum computer could, in theory, do as many calculations as you want – all at the same time.

Some describe this situation as multiple computers in parallel universes. Professor Seth Lloyd of MIT has a better analogy. He describes a quantum computer as being like a musical chord. You can hear several notes at the same time. A quantum system in coherence can have several states, each of which exists at the same time. Operating a quantum computer is like setting off a musical chord, and then tuning in to hear the dominant note – the answer.

It's obvious why this is so useful. A quantum computer as powerful as this could instantly crack any code. Codes rely on the fact that it is very hard to find the prime factors of a large number. For every digit added to a number, the amount of computing time required to crack it goes up exponentially. So, as conventional computers get faster, the computer industry can simply add a few more digits to the encryption key on a WiFi link or a secure webpage.

With a quantum computer, however, the time taken to solve the problem doesn't increase

exponentially. There's an algorithm created by Peter Shor, professor of mathematics at MIT, that, given a working quantum computer of a certain size, will crack a code that was previously uncrackable to all practical purposes.

But can we build a working quantum computer? If you remember Schrodinger's cat, you'll have guessed the drawback. Quantum systems are coherent only if isolated. Any noise or interaction with the outside world, and the quantum states collapse to one. A quantum computer stops working if you look at it.

To make a quantum computer, it seems, you must overcome three problems: building in enough qubits to build a computer faster than conventional systems; keeping the quantum computer isolated and coherent long enough to do actual work (the so-called decoherence time); and reading the quantum states at the end without destroying the result.

It's been slow going. Scientists have come up with various ways of making qubits, including optical components, trapped ions, quantum tunnelling and superconducting quantum interference devices (SQUIDs).

Quantum computing becomes really powerful only when you have many qubits, but scaling quantum computing experiments up to include more qubits has turned out to be difficult. This year, a couple of university projects have verified Shor's algorithm on systems of four qubits, but they are still far short of today's conventional computers.

The maximum number of qubits in any properly reviewed experiment has been 12, and those were not all coherent. This meant the qubits couldn't perform in the way quantum computing was originally envisaged, with all possible quantum states active.

There have been attempts to get longer decoherence times, but these are still only small fractions of a second – too short for useful work.

QUANTUM ENTANGLEMENT

With these limitations, researchers have had to devise very clever systems using quantum entanglement to get data in and out of a quantum computer. In quantum entanglement, the states of two particles depend on each other, even when they are separated.

Much attention has been paid to reading data from a quantum computer. Most methods accept that they can only arrive at the result with a certain level of probability, but techniques are evolving to push that level of probability higher.

There have been demonstrations of techniques that could lead to the creation of quantum cables. A team of researchers based in Quebec and Zurich created an 8mm linkage that can connect two SQUIDs. It's a small step, but it could allow qubits to connect to larger devices.

All this sounds disappointingly slow, but this is what happens when a subject is put into practice. Researchers started out in the hope that quantum computers could solve complex problems in one go, but as Umesh Vazirani, professor of computer science at Berkeley, pointed out in a letter to *The Economist*, "this mistaken view was put to rest in the infancy of quantum computation over a decade ago when it was established that the axioms of quantum physics severely restrict the type of information accessible during a measurement". It's still worth doing, he says, even though you don't get an exponential speed increase over classical computers.

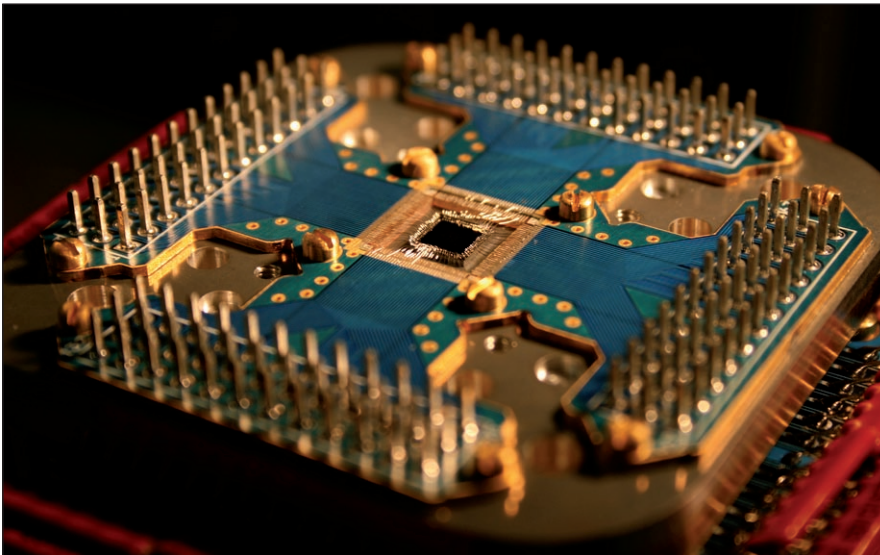
Others are gloomier. Michael Dyakonov of the University of Montpellier in France speculates that "since every qubit creates a greater opportunity for thermal noise, this makes the decoherence time shorter. Quantum computing could be more like perpetual motion – an absolute impossibility."

Lev Levitin and Tommaso Toffoli of Boston University suggested something similar in September 2007. Quantum computing is very sensitive to thermal noise, so any quantum computer designed to work reasonably fast will require extra qubits for redundancy and error correction. These requirements may cancel out the benefits of quantum computing, they argue.

Scott Aaronson, assistant professor of electrical engineering and computer science at MIT, has taken on board the difficulties, and goes back to the double-slit experiment for an explanation of what a real quantum computer might be: "The idea of quantum computing is to set up a massive double-slit experiment with exponentially many paths, and to try to arrange things so that the paths leading to wrong



▲ D-Wave's system must be kept at a very low temperature to keep its qubits in a superconducting state



▲ Orion may be a quantum processor, but it's built like an ordinary chip using micron-level lithography

answers interfere destructively and cancel each other out, while the paths leading to right answers interfere constructively and are therefore observed with high probability.”

A COMMERCIAL SYSTEM

Quantum computing doesn't lend itself to commercial funding. Even with the huge possible benefits, the pay-off is so far in the future that it isn't a good way for companies to spend too much of their money.

Companies such as IBM and HP have only dabbled in quantum computing. “A company that intends to be involved in the computational business a couple of decades from now should definitely be looking at quantum computation, but it is betraying its stockholders if it is currently spending more than a million dollars a year working on this area,” says Stan Williams, director of basic research for HP and founder of the company's quantum science research group.

Despite this, there is a commercial quantum computing company. D-Wave Systems, based in Canada, has raised \$44 million in venture

capital to fund its plan to deliver supercooled quantum computers to discerning (and rich) computer rooms in the next couple of years.

The company is the brainchild of maverick scientist Geordie Rose. Its approach uses adiabatic quantum computing (AQC), an alternative quantum computing technique described in a paper co-authored by Seth Lloyd.

Rose states on his website that the big benefit of AQCs is they don't need to be shut off from the world. “AQCs can be run in the presence of noise without quantum error correction, and still provide optimal scaling. In fact the thermal noise actually helps.”

An adiabatic quantum computer is designed to find the solution for one particular problem. When an AQC interacts with the outside world, its quantum systems settle to the state where they have the lowest energy, like a ball rolling downhill. An AQC is designed so that – for a given set of inputs – its lowest energy state is the answer to the problem.

A system's overall quantum state is called the Hamiltonian. This complex mathematical

function describes all the possible quantum values the system could have. It predicts the way the system will evolve over time. It dates back to 1833, when Irish mathematician William Rowan Hamilton rewrote classical mechanics, (including Newton's familiar laws of motion), as a set of equations. In classical physics, the Hamiltonian was a mathematical curiosity, showing underlying harmony and symmetry, but not very useful. In quantum mechanics, it turned out to be the only sensible way to express what is going on.

It is possible to define a system with a Hamiltonian such that the minimum energy state is the answer to the problem. An adiabatic quantum computer starts in a well-understood Hamiltonian, with the particles in their minimum energy state. Then the system is gradually changed to the new Hamiltonian. If the particles stay in their minimum energy states, the new Hamiltonian is also solved.

THERMAL POWER

So an AQC doesn't have a decoherence time, but it must be almost completely isolated from the world. A small amount of thermal energy jiggles it gently into its actual lowest energy state. The slow change from one state to another is sometimes referred to as ‘annealing’ – an analogy with the process by which metals are made stronger, by heating an amorphous lump gently, so that it can gradually crystallise into its stronger, lower-energy, crystalline form.

“Adiabatic quantum computing, properly understood, is real quantum computing,” says Professor Andrew Steane of Oxford University's Centre for Quantum Computing. “It is fully computationally equivalent to other forms of quantum computing, as long as it can be implemented in a general-purpose way with the right degree of control.”

The problem is achieving that control. An adiabatic quantum computer doesn't require total isolation, as other quantum computers do, but it's still pretty demanding. “I doubt this computing method is substantially easier to achieve than any other,” says Steane.



Unbreakable Quantum cryptography

Quantum computing may be controversial, but there's no doubt about the success of the related field of quantum cryptography. This uses quantum techniques to distribute cryptography keys that can guarantee secure communications, and will alert the user if anyone tries to intercept them.

Unlike quantum computing, quantum cryptography has been definitely demonstrated over a distance of more than 140km.

The problem with codes is in making sure that the people who are communicating have the keys, and no-one else. To make an unbreakable code, you simply combine your message with a unique string of characters that you use only once. Only someone who knows that string can read the message. But an unbreakable code is no use if an eavesdropper has the key.

There are two kinds of quantum cryptography. One uses Heisenberg's uncertainty principle and polarised photons, and the other uses quantum entanglement.

The polarised photon approach relies on the fact that, depending how you measure the polarisation of a photon of light, you get the right answer or a random answer. Light can be polarised in any direction, but this system uses just two pairs of states – rectilinear (horizontal or vertical) and diagonal (in two directions). The person sending the code creates a random string of 0s and 1s. For each bit, the sender makes a random choice between using the rectilinear or the diagonal scheme, and then sets the actual direction of polarisation according to a pre-agreed rule – so in the rectilinear scheme, for example, vertical represents 0 and horizontal represents 1. It doesn't matter if the eavesdropper knows this.

The receiver looks at each photon using polarising filters, either rectilinear or diagonal, which he picks at random. If he picks the right one, he can see which bit was encoded; if not, he inadvertently polarises the photon and gets a random digit, 0 or 1. At this point he doesn't know which digits are correct.

Once he has a string of digits, he transmits the polarisations he used (not the digits) and the sender does the same. It doesn't matter if an eavesdropper sees this, because the stream of bits is still private.

The two people throw out the bits where the receiver used the wrong polarisation, which leaves a string of digits they both know. There are refinements, but essentially, they know that no one has eavesdropped on them, because anyone observing the state of a photon will affect it.

Quantum entanglement is different. When two entangled photons are created, their polarisation must be opposite – but until it is measured, it's not determined (because of the principles of quantum mechanics). So if the photons are sent to two different people, when one is measured, the other will immediately take the opposite value. Again, there are refinements, but basically they end up with a string of bits that they can both agree on.



The other drawback is that AQCs solve only the problem they are designed for – they are specialised problem solvers and not general-purpose computers. It's possible to take a different problem and map it to the one the AQC solves, using conventional computers to turn it into an equivalent problem.

It's a bit like the way builders use the properties of string and gravity. With a weight tied to its end, the string is a simple machine that will find a vertical. But mediaeval builders mapped a more complex problem on to the same machine – a problem that today would warrant a computer-aided design tool.

The builders anchored the string at two points and let it hang freely. It formed a catenary curve, which is an upside-down image of the perfect load-bearing arch to go between those points. Just like the AQC, the string's solution is its lowest energy state, when it hangs still.

There's a limit to the number of building problems a catenary curve can solve, however, and there must also be a limit to the number of problems an AQC can solve, even with powerful conventional computers mapping them.

It seems that AQCs can't become universal code-breakers, but their advocates claim they can solve NP-complete problems. These are complex but useful problems where it is possible to guess right answers but very difficult to prove they are the best answer. Examples include the 'travelling salesman problem', in which a salesman with a list of customers has to plot the shortest route to all their addresses. It's easy to guess a route, but how would you prove there isn't a shorter one? Many optimisation problems also fall under the NP-complete category.

There are more lucrative NP-complete problems, such as maximising the return on an investment portfolio, or finding the stable shape of a protein molecule in drug design. D-Wave has chosen to solve one from thermodynamic theory, called the two-dimensional Ising problem. Any other NP-complete problem can be mapped to it, says Rose.

When pressed, Rose admits that D-Wave's AQC doesn't come up with an exact solution, but solves NP-complete problems "in the sense that it provides approximate solutions to things that are good enough in that they meet the requirements of the user".

It may be that no machine can completely solve them. "But that's an overly restrictive definition of what 'solving' means," says Rose. "Generally, if a business has one of these problems embedded in its daily operations, it uses what is called a heuristic to solve it, which is a set of rules of thumb that gives good approximate solutions quickly. Our machine has as its intended purpose competition with those heuristics."

IS IT REAL?

On these terms, how successful has D-Wave been? No-one actually knows – even though the company carried out public demonstrations in February and November 2007. Orion, the 16-qubit system that D-Wave built using \$44 million invested in the company, was shown over a live link from D-Wave's British Columbia lab to the Computer History Museum in Mountain View, California.

The Orion chip is built according to a well-established AQC design principle. Rings of superconducting niobium metal carry a current

in either direction or a superposition of both. They are etched on to a chip using standard micron-level lithography, and linked together to form the AQC. It has to be cooled to a few milliKelvin (just short of absolute zero), and doing that doesn't require leading-edge science. Sixteen qubits should be enough to handle 64,000 simultaneous inputs.

D-Wave pronounced the demonstration a success, describing the system as a "systems-level proof of concept". Orion was slower than a home PC, but it searched a database of protein structures, worked out a wedding seating plan and solved Sudoku puzzles.

Since then, D-Wave has posted a couple of papers to the ArXiv list of open-access physics papers, and issued some white papers to people willing to sign a non-disclosure agreement. A video of the event is available on restricted access on D-Wave's site. So far, no-one else has been allowed to test the device – despite a promise to make it available over the internet for other people to experiment with.

"Since the demo we have been developing the support infrastructure for our projects and have used it to design, build and test seven generations of processor prototypes," says Rose. "Each of these generations has focused on a specific issue related to performance and/or scalability of commercial processors."

At the Supercomputing 2007 show in Reno, Nevada, on 12th November, D-Wave demonstrated its quantum computer for the second time. Dr Hartmut Neven, Google's expert on image-searching, provided help with a demo algorithm for image searching. However, D-Wave has yet to publish the results or discuss them in depth. The scientific community is sceptical, partly for this reason and partly because the demonstration shows nothing that can't be achieved with conventional computers. Before the demonstration in Reno, Rose told us that "while the computing power is still not enough to compete with conventional silicon, it will run an application co-developed by an industrial partner".

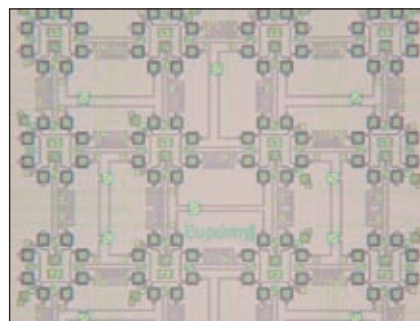
According to Rose, D-Wave is still on target to make a 1,000-qubit computer that can be integrated into conventional database systems in the third quarter of 2008.

WHAT'S IN THE BOX?

Professor Vazirani remains unconvinced, however. "D-Wave's demo consisted of a computer in a box that could solve simple problems. We have no way of knowing whether the computer in the box was an ordinary classical computer or a quantum computer."

Scott Aaronson doesn't believe that Orion will be very useful. In a talk given at Google's offices, he said: "They apparently built a device with 16 very noisy superconducting qubits." Qubits that are noisy – that let information into the environment – behave like classical bits, he points out. "It's consistent with the evidence that what D-Wave actually built would best be described as a 16-bit classical computer. I don't mean 16 bits in terms of the architecture; I mean 16 actual bits. There's some prior art for that."

In the world of peer-reviewed academic quantum computing experiments, it's rare to get two coherent superconducting qubits, so 16 would be a breakthrough. "In the absence of evidence from D-Wave that its 16 qubits are coherent, scientists are understandably



▲ The Orion processor contains 16 quantum bits wired together to solve a single problem

sceptical," says Vazirani. "If D-Wave's qubits are not coherent, as many scientists suspect, its computer would be classical, not quantum. This would still be consistent with the results of the demo, since the decohering qubits would act like classical random bits, and the adiabatic computer would act like a classical computer implementing simulated annealing, which would be quite fast for a small 16-bit Ising problem." D-Wave, says Vazirani, hasn't even bothered to test for coherence.

ALGORITHM BLUES

Vazirani is also scathing about the algorithm on D-Wave's Orion. "It wishes to use it to solve the Ising model, which is thought to be beyond the reach of classical computers," he says, "but there is no known efficient algorithm for solving the Ising model using this adiabatic approach."

"Quantum computing is an exciting field that has caught the imagination of the public," says Vazirani. "This is a good thing. But if the quantum computing effort starts to mingle fact with fiction, then the entire effort loses its credibility."

On one level, D-Wave's reticence is fair enough. After all, it is a commercial company, not a university, so it thrives on trade secrets and eventual sales, not citations. But at present, investors are asked to take a lot on faith.

This means that D-Wave's first quantum computer is itself something like a quantum paradox. It's sealed in a box marked 'secret'. In that box, there are two superposed states – a working quantum computer, and a disappointing phoney.

Until the box is opened, we won't know. **CS**

Further reading

Simple Quantum Physics by Peter Landshoff
(ISBN-13: 978-0521295383)

Paper by HP's Stan Williams
http://dwave.files.wordpress.com/2007/02/stan_williams_qc_investment.pdf

Geordie Rose's blog
<http://dwave.wordpress.com>

Scott Aaronson's blog
<http://scottaaronson.com/blog>

D-Wave
www.dwavesys.com

Cornell University Library
Open access to quantum computing papers
<http://arxiv.org>